

30.05.22

Note 1

9a902d381d8f4e4fb5ff8c1e77b38c57

Пусть G — непустое множество. $\{\{c1:: \text{Отображение вида}$

$$G \times G \rightarrow G$$

$\}\}$ называется $\{\{c2:: \text{бинарной операцией на множестве } G.\}\}$

Note 2

6fdd3ac4b4f644cea3704bcc79918836

Пусть $\{\{c1:: G \text{ — непустое множество,}\}\}$ $\{\{c2:: \circ \text{ — бинарная опера-$
ция на $G.\}\}$ $\{\{c4:: \text{Пара } (G, \circ)\}\}$ называется $\{\{c3:: \text{группой,}\}\}$ если $\{\{c4::$
она удовлетворяет аксиомам группы.\}

Note 3

827b57c3950c42b28c381d37a49ddf39

Сколько утверждений представлено в наборе аксиом из определения группы (G, \circ) ?

■ Три.

Note 4

f526d0257921478ca77a37b97abb9d06

Какова первая аксиома в наборе аксиом из определения группы (G, \circ) ?

■ Операция \circ ассоциативна.

Note 5

ce2298302937453e87e0cf850f17af90

Какова вторая аксиома в наборе аксиом из определения группы (G, \circ) ?

■ Для операции \circ существует нейтральный элемент.

Note 6

9f917456f2bf4fe6bf4e35f8042c9499

$\{\{c2:: \text{Нейтральный элемент}\}\}$ из определения группы (G, \circ) обычно обозначают $\{\{c1:: e.\}\}$

Note 7

3a8f693c011348fd9e88038d036a5b42

Пусть (G, \circ) — группа, $\{a \in G\}$. Элемент $\tilde{a} \in G$ называется обратным к a , если

$$a \circ \tilde{a} = \tilde{a} \circ a = e.$$

}}

Note 8

13c9853893a445d9a33db6823c3a5146

Какова третья аксиома в наборе аксиом из определения группы (G, \circ) ?

■ $\forall a \in G$ существует обратный к a элемент.

Note 9

5ba5e27ac8a9481eac4302c3159a6596

Пусть (G, \circ) — группа, $a \in G$. Обратный элемент к a обычно обозначают a^{-1} .

Note 10

9f4da30e71b1403a998b7c3fdf192252

Множество всех невырожденных $n \times n$ матриц над полем F вместе с операцией умножения называется общей линейной группой.

Note 11

27a09e6a00d14e859d7ad1d78a4f74a3

Общая линейная группа из $n \times n$ матриц над полем F обозначается $\text{GL}(n, F)$.

Note 12

2ed3e0b5ee424059ae3baeb77a99c828

Множество $\{A \in \text{GL}(n, \mathbb{R}) \mid \det A = 1\}$ вместе с операцией умножения называется специальной линейной группой.

Note 13

7b61df257fe7441fa69b9d03205e3c8c

Специальная линейная группа из $n \times n$ матриц над \mathbb{R} обозначается $\text{SL}(n)$.

Note 14

938182eaf5d84619bb5637604e70b54b

Пусть V — линейное пространство. Тогда

$$(V, \{\cdot + \cdot\}) — \{\cdot\} \text{-группа.}$$

Note 15

aff87807663a4a91b5401bdf6899fbf6

$$(\mathbb{Z}^n, \{\cdot + \cdot\}) — \{\cdot\} \text{-группа.}$$

Note 16

8ced218a1c26445e933dbfd17c1eaad6

Множество всех ортогональных $n \times n$ матриц над \mathbb{R} вместе с операцией умножения называется общей ортогональной группой.

Note 17

91b1cca934884832853d2b3b5ba12743

Общая ортогональная группа из $n \times n$ матриц над \mathbb{R} обозначается $O(n)$.

Note 18

eb84d3b2cf0c4432ad56a0dbdc8604af

Множество $\{A \in O(n) \mid \det A = 1\}$ вместе с операцией умножения называется специальной ортогональной группой.

Note 19

56e431becf842f4bb0c6b21484e440b

Специальная ортогональная группа из $n \times n$ матриц над \mathbb{R} обозначается $SO(n)$.

Note 20

5c9f837485594f04924f55f586958257

Пусть $K \subset \mathbb{R}^n$. Множество движений пространства \mathbb{R}^n , сохраняющих множество K , вместе с операцией умножения называется группой симметрий K .

Note 21

822e126f31c7481393a42cee53def0b6

Пусть $K \subset \mathbb{R}^n$. Группа симметрий K обозначается $\text{Sym } K$.

Note 22

809c8a8f790e4a2a998a4a8038c03971

Группа (G, \circ) называется $\{\{c2\}$ абелевой, $\}\}$ если $\{\{c1\}$ операция \circ коммутативна. $\}\}$

Note 23

e59ac970ec54461083354dae9eeb4047

Может ли группа иметь несколько нейтральных элементов?

■ Нет, нейтральный элемент единственен.

Note 24

13fee55238844118889a790b6e0c7e37

Пусть (G, \circ) — группа. Тогда если e и e' — нейтральные элементы для \circ , то $e = e'$. В чём основная идея доказательства?

■ Рассмотреть $e \circ e'$.

Note 25

afa616033db44cee8d39131bb90173bd

Пусть (G, \circ) — группа, $a \in G$. Может ли в G существовать несколько элементов, обратных к a ?

■ Нет, обратный элемент единственен.

Note 26

9fdcdce939af46639169bda602d721c5

Пусть (G, \circ) — группа, $a \in G$. Тогда если a^{-1} и \tilde{a} — обратные элементы к a , то $\tilde{a} = a^{-1}$. В чём основная идея доказательства?

■ Представить \tilde{a} как $\tilde{a} \circ (a \circ a^{-1})$.

Note 27

3db3d03590c84407bfb64b2a80b0e1c5

Пусть (G, \circ) — группа, $\{\{c2\}$ $a, b \in G$. $\}\}$ Тогда

$$(a \circ b)^{-1} = \{\{c1\}$$
 $b^{-1} \circ a^{-1}$. $\}\}$

Note 28

10144a83e52a4f5cbf0f96c818e229a5

Пусть (G, \circ) — группа, $\{\{c3: H \subset G.\}\}$ Тогда $\{\{c4: (H, \circ)\}\}$ называется $\{\{c2: \text{подгруппой группы } (G, \circ),\}\}$ если $\{\{c1: (H, \circ) \text{ является группой.}\}\}$

Note 29

9de4580c8d2545bcad2c525fe42930ec

Пусть (G, \circ) — группа, $H \subset G$. Выражение “ $\{\{c2: (H, \circ) \text{ является подгруппой } (G, \circ)\}\}$ ” обозначается $\{\{c1: \$

$$(H, \circ) \leq (G, \circ).$$

$\}\}$

Note 30

bd4835b2c522436fac41030bf6b13a66

Пусть (G, \circ) — группа, $\{\{c4: a \in G,\}\}$ $\{\{c3: n \in \mathbb{N}.\}\}$

$$\{\{c2: a^n\}\} \stackrel{\text{def}}{=} \{\{c1: \underbrace{a \circ \cdots \circ a}_{n \text{ раз}}\}\}$$

Note 31

2e41bce96a5249ca9d372d04f772b9b4

Пусть (G, \circ) — группа, $\{\{c2: a \in G.\}\}$

$$a^0 \stackrel{\text{def}}{=} \{\{c1: e.\}\}$$

Note 32

2cfa92bf39b847d4aa21d381a0d2c428

Пусть (G, \circ) — группа, $a \in G$, $n \in \mathbb{N}$.

$$\{\{c2: a^{-n}\}\} \stackrel{\text{def}}{=} \{\{c1: (a^{-1})^n.\}\}$$

Note 33

3994ad9b38154ec081e7042011939b50

Пусть (G, \circ) — группа, $\{\{c3: a \in G,\}\}$ $\{\{c2: \text{Порядком элемента } a\}\}$ называется $\{\{c1: \text{либо}$

$$\min \{n \in \mathbb{N} \mid a^n = e\}.$$

либо ∞ , если таких n не существует. $\}\}$

Note 34

78e264e39e824819ace538828da51d7c

Пусть (G, \circ) — группа, $a \in G$. $\{\{c2:: \text{Порядок элемента } a\}\}$ обозначается $\{\{c1:: \text{ord } a.\}\}$

Note 35

2e3b057efc1e40b1843700b41b2052b9

Пусть (G, \circ) — группа, $\{\{c3:: a \in G.\}\}$ $\{\{c1:: \text{Множество } \{a^k \mid k \in \mathbb{Z}\} \text{ с операций } \circ\}\}$ называется $\{\{c2:: \text{подгруппой } (G, \circ), \text{ порождённой элементом } a.\}\}$

Note 36

fd96a89fdb1b45559782a7213101e400

Пусть (G, \circ) — группа, $a \in G$. $\{\{c2:: \text{Подгруппа } (G, \circ), \text{ порождённая элементом } a,\}\}$ обозначается $\{\{c1:: \langle a \rangle.\}\}$

Note 37

54a6a6775d1940b09be51518008fabdc

Пусть (G, \circ) — группа, $a \in G$. Тогда если $\{\{c2:: \text{ord } a < \infty,\}\}$ то

$$\{\{c3:: (\langle a \rangle, \circ)\}\} \simeq \{\{c1:: (\mathbb{Z}_{\text{ord } a}, +).\}\}$$

Note 38

d83fe9abbbfca4fc99b99e08866cc83a9

Пусть (G, \circ) — группа, $a \in G$. Тогда если $\{\{c2:: \text{ord } a = \infty,\}\}$ то

$$\{\{c3:: (\langle a \rangle, \circ)\}\} \simeq \{\{c1:: (\mathbb{Z}, +).\}\}$$

06.06.22

Note 1

053e51258ecd4ca588d279e34a89a3d3

Пусть $(G, \circ), (H, *)$ – группы, $\{\{c3::f : G \rightarrow H.\}$ Отображение f называется $\{\{c2::\text{гомоморфизмом групп},\}$ если $\{\{c1::$

$$\forall a, b \in G \quad f(a \circ b) = f(a) * f(b).$$

$\}$

Note 2

5266d124dc1d4300b1204c6286b3e25e

Пусть $(G, \circ), (H, *)$ – группы, $f : G \rightarrow H$ – гомоморфизм. Тогда

$$f(e) = \{\{c1::e.\}$$

Note 3

6fa9d3c343dc4c9dbd8cee9c37bbac42

Пусть $(G, \circ), (H, *)$ – группы, $f : G \rightarrow H$ – гомоморфизм. Тогда

$$f(a^{-1}) = \{\{c1::f(a)^{-1}\} \quad \forall a \in G.$$

Note 4

181a648ef262451fb18b4237c6c7f429

Пусть $(G, \circ), (H, *)$ – группы, $f : G \rightarrow H$. Отображение f называется $\{\{c2::\text{изоморфизмом групп},\}$ если $\{\{c1::\text{оно является гомоморфизмом и биективно},\}$

Note 5

743a7ef3a0c045548f43006f58969493

$$\{\{c2::\mathbb{R}_+\}\} \stackrel{\text{def}}{=} \{\{c1:: \{x \in \mathbb{R} \mid x > 0\} \cdot\}$$

(не как в матане!)

Note 6

7618af52019f4c6bb8a64f426a797e41

$$\{\{c2::\overline{\mathbb{R}_+}\}\} \stackrel{\text{def}}{=} \{\{c1:: \{x \in \mathbb{R} \mid x \geq 0\} \cdot\}$$

(не как в матане!)

Note 7

7dd1206881114b28bc9ef9c14a7fd882

Пример изоморфизма групп (\mathbb{R}_+, \cdot) и $(\mathbb{R}, +)$.

|

$$f : x \mapsto \ln x.$$

Note 8

2ec8dcb4e81d40eebde4db2b2702daa4

Пусть $n \in \mathbb{N}$.

$$\mathbb{Z}_n \stackrel{\text{def}}{=}_{\{\{c1::[0 : n - 1].. \}}$$

Note 9

ae71026122c54154a213e03843c8abcb

Пусть $a, b \in \mathbb{Z}_n$.

$$a + b \stackrel{\text{def}}{=}_{\{\{c1::(a + b) \bmod n.. \}}$$

Note 10

e13a32abbb104cd09a57e8b5d9724d85

Пусть $n \in \mathbb{N}$. Тогда $_{\{\{c2::(\mathbb{Z}_n, +)\}}$ называется $_{\{\{c1::\text{группой выче-}\}}$
тов по модулю n .

Note 11

59141e88226b4a72937b611774af1733

Пусть $a \in \mathbb{Z}_n$. Тогда

$$a^{-1} =_{\{\{c1::(n - a) \bmod n.. \}}$$

Note 12

8e7c4384053947bc8f40faac3d3bc34f

Пусть (G, \circ) — группа, $a \in G$, $\text{ord } a < \infty$. Тогда

$$(\langle a \rangle, \circ) \simeq (\mathbb{Z}_{\text{ord } a}, +).$$

В чём основная идея доказательства?

Построить изоморфизм $\mathbb{Z}_{\text{ord } a} \rightarrow \langle a \rangle$, $k \mapsto a^k$.

Note 13

129a1bab504e409cb12b31bb2da9c1ff

Пусть (G, \circ) — группа, $a \in G$, $\text{ord } a < \infty$. Как показать, что $f : k \mapsto a^k$, $\mathbb{Z}_{\text{ord } a} \rightarrow \langle a \rangle$ — гомоморфизм?

Представить $f(k_1 + k_2)$ как $g^{k_1 + k_2 - l \cdot n}$, $l \in \{0, 1\}$.

Note 14

69b8b587049647ca85d7cdc871bebb05

Пусть (G, \circ) — группа, $a \in G$, $\text{ord } a < \infty$. Как показать, что $f : k \mapsto a^k$, $\mathbb{Z}_{\text{ord } a} \rightarrow \langle a \rangle$ — сюръекция?

Представить $a^p \in \langle a \rangle$ как $a^{l \cdot n + k_0}$.

Note 15

86c7386b47444f4cab166aecca358d5b

Пусть (G, \circ) — группа, $a \in G$, $\text{ord } a < \infty$. Как показать, что $f : k \mapsto a^k$, $\mathbb{Z}_{\text{ord } a} \rightarrow \langle a \rangle$ — инъекция?

$$k \neq l \implies a^{k-l} \neq e.$$

Note 16

326a83d344554cb38aab476534b6f5e8

Пусть (G, \circ) — группа, $a \in G$, $\text{ord } a = \infty$. Тогда

$$(\langle a \rangle, \circ) \simeq (\mathbb{Z}, +).$$

В чём основная идея доказательства?

Построить изоморфизм $\mathbb{Z} \rightarrow \langle a \rangle$, $k \mapsto a^k$.

Note 17

31fd624715c244b2ba453e6ffe19dd74

Пусть (G, \circ) — группа, $\llbracket c3 \rrbracket (H, \circ)$ — подгруппа, $g \in G$.

$$\llbracket c2 \rrbracket g \circ H \stackrel{\text{def}}{=} \llbracket c1 \rrbracket \{g \circ h \mid h \in H\}.$$

Note 18

ac542c349e5b43e886540f1f0e62bacc

Пусть (G, \circ) – группа, (H, \circ) – подгруппа, $g \in G$.

$$\{c2: H \circ g\} \stackrel{\text{def}}{=} \{c1: \{h \circ g \mid h \in H\}.\}$$

Note 19

20affff668b04e9e80ea15dc66eab2c2

Пусть (G, \circ) – группа, (H, \circ) – подгруппа, $g \in G$. Множество $g \circ H$ называется левым классом смежности элемента g по подгруппе H .

Note 20

ca40d5b36a764e62924dfd73ea9ebc66

Пусть (G, \circ) – группа, (H, \circ) – подгруппа, $g \in G$. Множество $H \circ g$ называется правым классом смежности элемента g по подгруппе H .

Note 21

810cc5be7cb2498280729b27d347be4f

Пусть (G, \circ) – группа, (H, \circ) – подгруппа, $a, b \in G$.

$$\{c2: a \equiv b \pmod{H}\} \stackrel{\text{def}}{\iff} \{c1: a \circ b^{-1} \in H.\}$$

Note 22

ff25dee3ae6f4b1ab34700578cceaed5

Пусть (G, \circ) – группа, (H, \circ) – подгруппа, $a, b \in G$. Тогда

$$\{c2: a \equiv b \pmod{H}\} \iff \{c1: a \circ H = b \circ H.\}$$

(в терминах классов смежности)

Note 23

489a77d7bd2a4523886a65a220d953f4

Пусть (G, \circ) – группа, (H, \circ) – подгруппа. Отношение

$$\cdot \equiv \cdot \pmod{H}$$

является отношением эквивалентности.

Note 24

a07284200e0b4649bb1357b2aef3cc0

Пусть (G, \circ) — группа, (H, \circ) — подгруппа. Как показать, что отношение $\cdot \equiv \cdot \pmod{H}$ является симметричным?

$$a \circ b^{-1} \in H \implies (a \circ b^{-1})^{-1} \in H.$$

Note 25

745cc90590ef4d0784af24f93c539a9f

Пусть (G, \circ) — группа, (H, \circ) — подгруппа, $\{g_1, g_2 \in G\}$. Тогда всегда $g_1 \circ H$ и $g_2 \circ H$ либо не пересекаются, либо совпадают.

Note 26

020ff9f58e534258a0a8999bfff4003f6

Пусть (G, \circ) — группа, (H, \circ) — подгруппа, $g_1, g_2 \in G$. Тогда всегда $g_1 \circ H$ и $g_2 \circ H$ либо не пересекаются, либо совпадают. В чём ключевая идея доказательства?

Показать, что если $g_1 \circ H$ и $g_2 \circ H$ пересекаются, то они совпадают как множества.

Note 27

2bafb8136a75400481ba0f463cb2dc9c

Пусть (G, \circ) — группа, (H, \circ) — подгруппа, $g \in G$. Тогда количество элементов в $g \circ H$ равно количеству элементов в H .

Note 28

7d8237766a784691b937e2a028a32f28

Пусть (G, \circ) — группа, (H, \circ) — подгруппа, $g \in G$. Тогда количество элементов в $g \circ H$ равно количеству элементов в H . В чём ключевая идея доказательства?

Показать, что $g \circ h \mapsto h$ — биекция.

Note 29

45bd2c9c51fd4a398ac4ada9172dfc6

Пусть (G, \circ) — группа. Количество элементов в G называется порядком группы (G, \circ) .

Note 30

0590e16f8b204e27a704de1a4d810d76

Пусть (G, \circ) — $\{\{c3::\text{конечная группа},\}\}$ $\{\{c2::(H, \circ) — \text{подгруппа},\}\}$
 Тогда $\{\{c1::\text{порядок группы } G \text{ делится на порядок группы } H.\}\}$

« $\{\{c4::\text{Теорема Лагранжа}\}\}$ »

Note 31

6bbf33cf39f34f34afa5cf2be59fd219

В чём основная идея доказательства теоремы Лагранжа для конечных групп?

Представить G как конечное объединение непересекающихся классов смежности $g_i \circ H$.

Note 32

daf66fd18e1b4e50b007b6a820bfc2b7

Пусть (G, \circ) — группа, (H, \circ) — подгруппа. Подгруппа (H, \circ) называется $\{\{c2::\text{нормальной},\}\}$ если $\{\{c1::$

$$\forall g \in G \quad g \circ H = H \circ g.$$

$\}\}$

Note 33

7fa9d6859025408f868211197328bf30

Пусть (G, \circ) — группа, $\{\{c3::(H, \circ) — \text{нормальная подгруппа},\}\}$
 $a, b \in G$. Тогда

$$\{\{c2::(a \circ H) \cdot (b \circ H)\}\} \stackrel{\text{def}}{=} \{\{c1::(a \circ b) \circ H\}\}$$

Note 34

94d010d0ee6748df9997775ed206113d

Пусть (G, \circ) — группа, (H, \circ) — подгруппа. Тогда если $\{\{c3::(H, \circ) — \text{нормальная подгруппа},\}\}$ то

$$\{\{c2::(\{g \circ H \mid g \in G\}, \cdot)\}\} — \{\{c1::\text{группа},\}\}$$

Note 35

f8a3768ad050440ab84f132b57ff2665

Пусть (G, \circ) — группа, (H, \circ) — подгруппа. Тогда если (H, \circ) — нормальная подгруппа, то

$$(\{g \circ H \mid g \in G\}, \cdot) \text{ — группа.}$$

Почему важно, что (H, \circ) — нормальная подгруппа?

В противном случае операция умножения может не быть корректно определённой.

Note 36

6df4f13013d04e2d81bc271465e769b9

Пусть (G, \circ) — группа, (H, \circ) — нормальная подгруппа. Группа классов смежности по подгруппе H называется фактор группой группы (G, \circ) по подгруппе H .

Note 37

30b68180adac4dab81ea034157975d43

Пусть (G, \circ) — группа, (H, \circ) — нормальная подгруппа. Фактор группа (G, \circ) по подгруппе H обозначается

$$G/H.$$

}}

Note 38

ce44f6c96679478284d511f7a3be6f0e

$$\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}.$$

Note 39

9f1bb49a26844d51a59a5c4aac626fa9

Как показать, что $f : k \mapsto k + n\mathbb{Z}, \mathbb{Z}_n \rightarrow \mathbb{Z}/n\mathbb{Z}$ — биекция?

Из теоремы о делении с остатком определить f^{-1} .

Note 40

723eb2544eda4ac2837ba4d68c85f327

$$\mathbb{S}^1 \stackrel{\text{def}}{=} \{z \in \mathbb{C} \mid |z| = 1\}.$$

Note 41

51f563718c3046b49cc18008a09f772e

$$(\mathbb{R}/\mathbb{Z}, +) \simeq_{\{\{c1::(\mathbb{S}^1, \cdot)\}\}} (\mathbb{S}^1, \cdot)$$

Note 42

54c093c580df4acab83f28d38696caf0

$(\mathbb{R}/\mathbb{Z}, +) \simeq (\mathbb{S}^1, \cdot)$. В чём ключевая идея доказательства?

| $x + \mathbb{Z} \mapsto e^{i \cdot 2\pi x}$ — изоморфизм с тривиальным обратным отображением.

Семинар 01.06.22

Note 1

36d221e9357e4a0cb1335c1926abeca7

Множество $\sqrt[n]{1}$ образует $\{\{c2::\text{группу}\}\}$ относительно $\{\{c1::\text{умно- жения.}\}\}$

Note 2

451622b7a7564fc4aa814dd526055fe6

Множество $\bigcup_n \sqrt[n]{1}$ образует $\{\{c2::\text{группу}\}\}$ относительно $\{\{c1::\text{умно- жения.}\}\}$

Note 3

6c7fab41a91e4d339555af9508593e91

Пусть (G, \circ) – группа, $a \in G$. Тогда количество элементов в $\{\{c2::\langle a \rangle\}\}$ равно $\{\{c1::\text{ord } a.\}\}$

Note 4

f0e23db5db674658b20e95a3c304e1c7

Пусть (G, \circ) – группа, $a \in G$. Тогда

$$\text{ord}(a^{-1}) = \{\{c1:: \text{ord } a.\}\}$$

Note 5

95b9c2ecea204819ba17ec6952a3cafd

Пусть (G, \circ) – группа, $a \in G$. Тогда

$$a^{-n} = e_{\{\{c2:: \iff \}\}\{\{c1:: a^n = e.\}\}}$$

Note 6

b9e7bf38ba554ac89a7dbe249ac1a0ca

Пусть (G, \circ) – группа, $a \in G$, $\{\{c3:: \text{ord } a = n,\}\}$ $k \in \mathbb{N}$. Тогда

$$\{\{c2:: \text{ord}(x^k)\}\} = \{\{c1:: \frac{n}{\text{gcd}(n, k)}.\}\}$$

Note 7

897a73a19e0545d5a480f6d1da8c3584

Пусть (G, \circ) – группа, $a \in G$, $\text{ord } a = n$, $k \in \mathbb{N}$. Тогда

$$\text{ord}(x^k) = \frac{n}{\gcd(n, k)}.$$

В чём основная идея доказательства?

|

$$a^{kp} = a^{\alpha n} \implies p = \frac{\alpha n}{k}.$$

Note 8

50e7ebab24cf4ba7b56cba450b2ee6ed

Пусть $(\langle a \rangle, \circ)$ – циклическая группа порядка n , $\{k \mid n\}$
Тогда

$$\left\{ g \in \langle a \rangle \mid g^k = e \right\} = \left\{ a^{\frac{pn}{k}} \mid p \in [0 : k - 1] \right\}.$$

Note 9

a2f886f5a18747b3be104ae46fbc7bf

Пусть $(\langle a \rangle, \circ)$ – циклическая группа порядка n , $\{k \mid n\}$
Тогда

$$\text{ord}\left(a^{\frac{pn}{k}}\right) = k \iff \gcd(p, k) = 1.$$